IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

KARA ZILER and A.L.S., a minor, through her parent and legal guardian Linda Stanton, individually and on behalf of all others similarly situated, Plaintiffs, v. EAST TENNESSEE CHILDREN'S HOSPITAL ASSOCIATION, INC., Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Kara Ziler and A.L.S., a minor, through her parent and legal guardian, Linda Stanton ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their undersigned attorneys, bring this Class Action Complaint against Defendant East Tennessee Children's Hospital Association, Inc. ("ETCH") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against ETCH for its failure to secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") of approximately 422,531 ETCH patients, including Plaintiffs. The data reportedly exposed in the breach includes the most sensitive types of data that cyber criminals and fraudsters seek in order to commit fraud and identity theft. According to ETCH, information disclosed in the breach

includes names, contact information, dates of birth, medical record numbers, medical history information, and Social Security numbers.

2. Defendant ETCH is one of four Comprehensive Regional Pediatric Centers in Tennessee.[1] As the primary provider of pediatric care in East Tennessee, ETCH "offers the services of many different pediatric subspecialties."[2]

3. On or about March 18, 2022, ETCH determined that unauthorized individuals had gained access to its network systems and had access to the PII/PHI of Plaintiffs and Class members between March 11, 2022, and March 14, 2022 (the "Data Breach").

4. ETCH owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. ETCH breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

5. As a result of ETCH's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach, which ETCH learned of on or about March 14, 2022, and first publicly acknowledged on or about May 19, 2022.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust

[1] *About Us*, EAST TENNESSEE CHILDREN'S HOSPITAL, https://www.etch.com/about-us/ (last visited May 31, 2022).

[2] *Id.*

enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Kara Ziler is a Tennessee resident. She is a former patient at ETCH or has otherwise transacted with and provided her PII/PHI to ETCH. In May 2022, Plaintiff Ziler received a letter from ETCH notifying her that her PII/PHI may have been exposed in the Data Breach. The letter identified that Plaintiff Ziler's PII/PHI was compromised in the Data Breach. As a result of the Data Breach and after receiving the breach notice letter, Plaintiff Ziler has spent approximately 3 hours monitoring her accounts for fraud to ensure she does not become the victim of fraud or identity theft.

8. Plaintiff A.L.S., a minor, and her mother and legal guardian Linda Seaton are Tennessee residents. Plaintiff A.L.S. is a current patient at ETCH or has otherwise provided her PII/PHI to ETCH. In May 2022, Plaintiff A.L.S. received a letter from ETCH notifying her that her PII/PHI may have been exposed in the Data Breach. The letter identified that Plaintiff A.L.S.'s PII/PHI was compromised in the Data Breach. As a result of the data breach, Plaintiff A.L.S. has been exposed to harm and imminent risk of identity theft and fraud. Furthermore, Ms. Seaton has lost several hours of time undertaking efforts to mitigate potential fraud and identity theft relating to her minor child.

9. Defendant East Tennessee Children's Hospital is incorporated in Tennessee and is located at 2018 W Clinch Avenue, Knoxville, Tennessee 37916.

JURSDICTION AND VENUE

10. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a

citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

11. This Court has personal jurisdiction over ETCH because ETCH is a corporation organized under the laws of Tennessee.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because ETCH's principal place of business is located in Knoxville, Tennessee.

FACTUAL ALLEGATIONS

Overview of ETCH

13. Founded in 1937, ETCH is one of four Comprehensive Regional Pediatric Centers in Tennessee.[3] The hospital's specialists provide a wide range of pediatric services ranging from routine care, such as ear tube placement surgeries and tonsillectomies, to highly specialized services, including treatment for cancer, blood disorders, and other diseases that afflict children and adolescents. ETCH has approximately 160,000 patient visits annually.[4]

14. In the regular course of its business, ETCH collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services.

15. ETCH requires patients to provide personal information before it provides them services. That information includes names, addresses, dates of birth, health insurance information, and Social Security numbers.

16. Plaintiffs and Class members are, or were, patients of ETCH or received health-related or other services from ETCH, and entrusted ETCH with their PII/PHI.

---

[3] *See* n.1, *supra*.

[4] *History of East Tennessee Children's Hospital*, EAST TENNESSEE CHILDREN'S HOSPITAL, https://www.etch.com/about-us/history-of-east-tennessee-childrens-hospital/ (last visited May 31, 2022).

17. ETCH acknowledges its responsibility to protect Plaintiffs' and other Class members' PHI. In its Privacy Policy, ETCH confirms that "It is our responsibility to safeguard your child's protected health information."[5] Despite this acknowledgment and the assertions and implicit promises in its Privacy Policy to safeguard PHI, ETCH failed and fails to do so.

The Data Breach

18. In a statement posted on ETCH's website on March 14, 2022, ETCH indicated that it experienced an "information technology security issue in the evening hours of Sunday, March 13, 2022."[6]

19. On May 19, 2022, over two months following its initial statement, ETCH posted a Notice of Data Incident on its website, stating that ETCH first "identified unusual activity on its network" on or about March 13, 2022, and "commenced a comprehensive investigation into the incident" at that time. [7]

20. On March 18, 2022, ETCH determined that "certain documents stored within ETCH's environment may have been copied from or viewed on the system by an unauthorized person(s) between March 11, 2022, and March 14, 2022."[8] According to ETCH, it "then undertook a comprehensive review of the affected data to determine what records were present and to whom

[5] *Privacy Policy*, EAST TENNESSEE CHILDREN'S HOSPITAL, https://www.etch.com/privacy/ (last visited May 31, 2022).

[6] *East Tennessee Children's Hospital Statement on Security Issue*, EAST TENNESSEE CHILDREN'S HOSPITAL, https://www.etch.com/about-us/news/2022/east-tennessee-childrens-hospital-statement-on-security-issue/ (March 14, 2022).

[7] *East Tennessee Children's Hospital Provides Notice of a Data Incident*, EAST TENNESSEE CHILDREN'S HOSPITAL, https://www.etch.com/about-us/news/2022/notice-of-data-incident/ (May 19, 2022).

[8] *Id*.

the information related" and that, on April 19, 2022, the investigation determined that certain patient information was present in the affected data."[9]

21. ETCH began to notify its patients of these alleged facts on or about May 19, 2022, via the Notice of Data Incident on its website, and the Notice of Security Incident letters that ETCH provided to impacted persons. ETCH stated that the information that was accessed included names, contact information, dates of birth, medical record numbers, medical history information, and Social Security numbers.

ETCH Knew That Criminals Target PII/PHI

22. At all relevant times, ETCH knew, or should have known, its patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, ETCH failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that ETCH should have anticipated and guarded against.

23. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company, Protenus, found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[10] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[11]

24. PII/PHI is a valuable property right.[12] The value of PII/PHI as a commodity is

---

[9] *Id*.

[10] *2021 Breach Barometer*, PROTENUS, https://www.protenus.com/resources/2021-breach-barometer (last visited May 30, 2022).

[11] *2020 Breach Barometer*, PROTENUS, https://www.protenus.com/resources/2020-breach-barometer (last visited May 30, 2022).

[12] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well

measurable.[13] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[15] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

25. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

26. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[16] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[17] A study by Experian found that the

---

understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[13] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[14] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[15] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[16] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[17] *Id.*

"average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[18]

27. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[19] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[20]

28. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[21] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[22]

29. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies

---

[18] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[19] SC Staff, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[20] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[21] *See* n.16, *supra*.

[22] *Id.*

confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

31. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[24]

32. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[25] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card

---

[23] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*: *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[24] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited May 31, 2022).

[25] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

number to withdraw funds, obtain a new driver's license or ID, or use the victim's information in the event of arrest or court action.[26]

33. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[27]

34. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[28]

35. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[26] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[27] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 26, 2022).

[28] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends And Workplaces*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited May 26, 2022).

36. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[29]

37. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[30] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[31] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [32] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[33]

38. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and

[29] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[30] Pam Dixon and John Emerson, *Report: The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

[31] *See* n.20, *supra*.

[32] *See* n.24, *supra*.

[33] *Id*.

corrected.

- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[34]

39. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[35]

40. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[34] *See* n.30, *supra*.

[35] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

Damages Sustained by Plaintiffs and the Other Class Members

41. Plaintiffs sand all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

42. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

43. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All persons whose PHI/PII was accessed by unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

44. Excluded from the Class is ETCH and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

45. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

46. The members in the Class are so numerous that joinder of all Class members in a

single proceeding would be impracticable. ETCH reported to the Maine Attorney General that approximately 422,531 individuals' information was exposed in the Data Breach.[36]

47. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

A. Whether ETCH had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;

B. Whether ETCH failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;

C. Whether an implied contract existed between Class members and ETCH providing that ETCH would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

D. Whether ETCH breached its duties to protect Plaintiffs' and Class members' PII/PHI; and

E. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

48. ETCH engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

---

[36] *Data Breach Notifications*, OFFICE OF THE MAIN ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/46d9b313-945c-45ac-a319-604a44439aa8.shtml (last visited May 31, 2022).

49. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by ETCH, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

50. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that Plaintiffs have no interests adverse to, or that conflict with, the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

51. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against ETCH, so it would be impracticable for Class members to individually seek redress from ETCH's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

52. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

53. ETCH owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

54. ETCH knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. ETCH knew of the many data breaches that targeted healthcare providers in recent years.

55. Given the nature of ETCH's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, ETCH should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

56. ETCH breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

57. It was reasonably foreseeable to ETCH that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

58. But for ETCH's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

59. As a result of ETCH's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II

NEGLIGENCE PER SE

60. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

61. ETCH's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

62. ETCH's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as ETCH, of failing to employ reasonable measures to protect and secure PII/PHI.

63. ETCH violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. ETCH's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

64. ETCH's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

65. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

66. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

67. It was reasonably foreseeable to ETCH that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

68. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of ETCH's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III

BREACH OF FIDUCIARY DUTY

69. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

70. Plaintiffs and Class members gave ETCH their PII/PHI in confidence, believing that ETCH would protect that information. Plaintiffs and Class members would not have provided ETCH with this information had they known it would not be adequately protected. ETCH's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between ETCH and Plaintiffs and Class members. In light of this relationship, ETCH must act primarily for the benefit of its patients and former patients, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

71. ETCH has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

72. As a direct and proximate result of ETCH's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in ETCH's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV

BREACH OF IMPLIED CONTRACT

73. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

74. In connection with receiving medical services, Plaintiffs and all other Class members entered into implied contracts with ETCH.

75. Pursuant to these implied contracts, Plaintiffs and Class members paid money to ETCH, whether directly or through their insurers, and provided ETCH with their PII/PHI. In

exchange, ETCH agreed to, among other things, and Plaintiffs understood that ETCH would: (1) provide medical services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and (3) protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

76. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and ETCH, on the other hand. Indeed, as set forth *supra*, ETCH recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Notice. Had Plaintiffs and Class members known that ETCH would not adequately protect its patients' and former patients' PII/PHI, they would not have received medical services from ETCH.

77. Plaintiffs and Class members performed their obligations under the implied contract when they provided ETCH with their PII/PHI and paid—directly or through their insurers—for health care services from ETCH.

78. ETCH breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

79. ETCH's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

80. Plaintiffs and all other Class members were damaged by ETCH's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V

UNJUST ENRICHMENT

81. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

82. This claim is pleaded in the alternative to the breach of implied contract claim.

83. Plaintiffs and Class members conferred a monetary benefit upon ETCH in the form of monies paid for healthcare services or other services.

84. ETCH accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. ETCH also benefitted from the receipt of Plaintiffs' and Class members' PHI, as this was used to facilitate payment.

85. As a result of ETCH's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members

paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

86. ETCH should not be permitted to retain the money belonging to Plaintiffs and Class members because ETCH failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

87. ETCH should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against ETCH as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent ETCH from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 1, 2022

Respectfully submitted,

/s/ *Kevin H. Sharp*

Kevin H. Sharp, BPR No. 016287
Leigh Anne St. Charles, BPR No. 036945
SANFORD HEISLER SHARP, LLP
611 Commerce Street, Suite 3100
Nashville, TN 37203
Telephone: (615) 434-7000
Facsimile: (615) 434-7020
ksharp@sanfordheisler.com
lstcharles@sanfordheisler.com

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

TINA WOLFSON*
twolfson@ahdootwolfson.com
ROBERT AHDOOT*
rahdoot@ahdootwolfson.com

AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
RILEY W. PRINCE*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: 312.621.2000
Facsimile: 312.641.5504

**pro hac vice* to be submitted